

On the Success of Mishandling Euclid's Lemma

ADRIAN W. DUDEK
Mathematical Sciences Institute
The Australian National University
adrian.dudek@anu.edu.au

Abstract

We examine Euclid's lemma that if p is a prime number such that $p|ab$, then p divides at least one of a or b . Specifically, we consider the common misapplication of this lemma to numbers that are not prime, as is often made by undergraduate students. We show that a randomly chosen implication of the form $r|ab \Rightarrow r|a$ or $r|b$ is *almost surely* false in a probabilistic sense, and we quantify this with a corresponding asymptotic formula.

I recently gave a tutorial to my undergraduate number theory class, wherein a severe warning was issued. Specifically, I told them that Euclid's lemma states that if p is a prime and $p|ab$, then p divides at least one of a and b (see Theorem 3 of Hardy and Wright [1]). I followed this with words of warning, grimly telling them that many students seem to let slip the all-important premise that p must be prime. They nodded with spirit – as undergraduate students often do – but unfortunately and in spite of my stern words, a suite of assignments now sit on my desk, where Euclid's lemma has been heartily applied in the case where p is not a prime. That is, many have incorrectly supposed that given any old divisor r of the product ab , it must be the case that r divides at least one of a and b .

Of course, such an implication can sometimes be true, but is certainly not true in general (take, for example, $r = 6$, $a = 2$ and $b = 3$). In fact, it is the purpose of this short article to show that a randomly chosen implication of the form

$$r|ab \Rightarrow r|a \text{ or } r|b$$

is *almost surely* false, that is, the probability of it being true is zero. Moreover, we furnish an asymptotic formula which quantifies this exactly.

Theorem 1. *Let $B(N)$ count the number of triples (a, b, r) of positive integers such that $r|ab$ and $ab \leq N$, and let $A(N)$ count the number of these triples such that r divides at least one of a and b . Then we have that*

$$\frac{A(N)}{B(N)} \sim \frac{\pi^2}{\log N}$$

as $N \rightarrow \infty$.

First, let's calculate $B(N)$. As usual, we let $d(n)$ denote the number of divisors of n . As $B(N)$ counts the number of triples (a, b, r) such that $r|ab$ and $ab \leq N$, it is clear that

$$B(N) = \sum_{ab \leq N} d(ab)$$

where the sum is over all a and b with $ab \leq N$. Therefore, we have that

$$\begin{aligned} B(N) = \sum_{ab \leq N} d(ab) &= \sum_{n \leq N} \sum_{ab=n} d(ab) \\ &= \sum_{n \leq N} d(n)^2 \\ &= \pi^{-2} N \log^3 N + O(N \log^2 N) \end{aligned}$$

by a result of Ramanujan [2].

We now wish to bound $A(N)$. Writing this as

$$A(N) = \sum_{ab \leq N} \sum_{r|ab} 1_{\{r|a \text{ or } r|b\}},$$

we first want to bound the number of divisors r of ab such that r divides at least one of a and b . Now, inclusion-exclusion gives us, for fixed integers a and b , that

$$\sum_{r|ab} 1_{\{r|a \text{ or } r|b\}} = d(a) + d(b) - \sum_{\substack{r|a \\ r|b}} 1.$$

It follows immediately that

$$A(N) = \sum_{ab \leq N} (d(a) + d(b)) - \sum_{ab \leq N} \sum_{\substack{r|a \\ r|b}} 1. \quad (1)$$

We will bound the sum on the right in the following lemma.

Lemma 2. *We have that*

$$\sum_{ab \leq N} \sum_{\substack{r|a \\ r|b}} 1 = O(N \log N).$$

Proof. Note that we are summing over all positive integers rc and re such that $r^2 ce \leq N$. Thus, we have that

$$\sum_{ab \leq N} \sum_{\substack{r|a \\ r|b}} 1 = \sum_{r \leq N} \sum_{rc \leq N} \sum_{re \leq N/rc} 1,$$

where the second and third summations are over c and e respectively. Using the fact that $\sum_{n \leq x} n^{-1} = \log x + O(1)$, we have that

$$\begin{aligned} \sum_{r \leq N} \sum_{rc \leq N} \sum_{re \leq N/rc} 1 &= \sum_{r \leq N} \sum_{c \leq N/r} \left(\frac{N}{r^2 c} + O(1) \right) \\ &= N \sum_{r \leq N} \frac{\log(N/r)}{r^2} + O(N \log N) \\ &= N \log N \sum_{r \leq N} \frac{1}{r^2} - N \sum_{r \leq N} \frac{\log r}{r^2} + O(N \log N) \end{aligned}$$

Noting that both of the sums in the above equation are $O(1)$ completes the proof. \square

Remark 1. *From the fact that $r|a$ and $r|b$ if and only if $r|\gcd(a, b)$, it follows that the sum in Lemma 2 is equal to*

$$\sum_{ab \leq N} d(\gcd(a, b)).$$

It would be interesting to see an asymptotic formula for this.

Now, from the symmetry of divisors, (1) and the above lemma, it follows that

$$\begin{aligned} A(N) &= 2 \sum_{ab \leq N} d(a) + O(N \log N) \\ &= 2 \sum_{b \leq N} \sum_{a \leq N/b} d(a) + O(N \log N). \end{aligned}$$

Using the classic bound (see Theorem 320 of [1])

$$\sum_{n \leq N} d(n) = N \log N + O(N),$$

we have that

$$\begin{aligned} A(N) &= 2 \sum_{b \leq N} \left(\frac{N}{b} \log \frac{N}{b} + O\left(\frac{N}{b}\right) \right) + O(N \log N) \\ &= 2N \log N \sum_{b \leq N} \frac{1}{b} - 2N \sum_{b \leq N} \frac{\log b}{b} + O(N \log N). \end{aligned}$$

By comparison to the integral, we can estimate the middle sum *viz.*

$$\begin{aligned} \sum_{b \leq N} \frac{\log b}{b} &= \int_1^N \frac{\log t}{t} dt + O\left(\frac{\log N}{N}\right) \\ &= \frac{\log^2 N}{2} + O\left(\frac{\log N}{N}\right). \end{aligned}$$

It follows that

$$A(N) = N \log^2 N + O(N \log N)$$

and this completes the proof of Theorem 1.

Acknowledgements

The author is gracious of the financial support provided by an Australian Postgraduate Award and an ANU Supplementary Scholarship. He would also like to thank the anonymous referees for providing useful feedback, and his number theory class for accidentally motivating the result of this paper.

References

- [1] G. H Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, 6th edition, 2008.
- [2] S. Ramanujan. Some formulae in the analytic theory of numbers. *Messenger of Math.*, 45:81–84, 1915.